EC-2000-007
IV-D-137

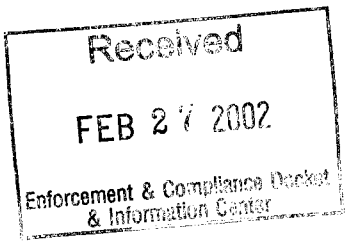
STATE OF MICHIGAN
DEPARTMENT OF ENVIRONMENTAL QUALITY
LANSING

JOHN ENGLER
GOVERNOR

RUSSELL J. HARDING
DIRECTOR

February 8, 2002

United States Environmental Protection Agency
Enforcement and Compliance Docket
and Information Center, (Mail Code 2201A)
1200 Pennsylvania Avenue NW
Washington, DC 20460



ATTENTION: Docket Number EC-2000-007

Dear Sir or Madam:

The Michigan Department of Environmental Quality (MDEQ) has reviewed the U.S. Environmental Protection Agency's (EPA) proposed Rule, 40 CFR Part 3, Cross-Media Electronic Reporting and Record Keeping Rule (CROMERRR) and has the following comments.

Rule Benefits

In general, the intent of the CROMERRR is acceptable but it contains a few notable flaws. This is a positive move by the EPA to draft a performance-based rather than technology-based policy. This reflects the state's perspective that a technology-neutral rule allows for flexibility which should facilitate the reporting process and serve as an incentive for industry participation.

Two of the most notable flaws pertain to (1) record keeping, and (2) use of digital signatures based on Public Key Infrastructure (PKI) certificates. The later issue in particular appears to contradict EPA's stated intent of creating a performance-based rather than a technology-based policy. These two issues need to be addressed if electronic submission of environmental information is to become a reality between the regulated community and the regulators.

Subpart A – General Provisions

3.1(a) – It appears that the intent of the rule is applicable to routine compliance reporting and other electronic records. It is not clear if this rule will apply to the submission of permit applications. The EPA should clarify in the preamble whether this rule is applicable to electronically submitted permit applications.

3.2(b) – The language in the rule does not appear to prohibit the use of printed paper records for record keeping purposes even if the original was derived from electronic (digital) data acquisitions systems. The EPA should clearly state that electronic records

created from automated recorders and other electronic data gathering systems and electronic data used to populate electronic reports are not applicable to the record keeping requirements. Only the final electronic record created for submission should be subject to this rule.

Subpart B – Electronic Reporting to EPA

3.10(a) – The rule must ensure that an electronic document submitted to the Central Data Exchange or other designated electronic document receiving system as designated under S.3.10(b) must be subject to the same criteria as those specified in the CROMERRR. Failure to do so may result in challenges to the rule's credibility and enforceability. It may also contribute to electronic reporting problems and confusion for companies with facilities in both delegated and non-delegated states, due to differing performance requirements.

Subpart C – Electronic Record Keeping under EPA Programs

3.100(a) - The electronic record keeping requirements appear to be reasonable and necessary for State record keeping systems. However, it could be very costly if each regulated entity was required to independently modify their systems to meet the required record keeping capability. The record keeping function should be provided by the delegated agency, which would ensure a consistent standard and reduce development costs.

We feel strongly that the proposed rule will create "additional" record keeping requirements which are far beyond what are required in the current regulations, i.e. paper systems. Such requirements will make the rule impractical and near impossible to implement by both the states and the regulated community. Current environmental regulations require the industry to keep records of the submissions and, in certain cases, information used to either generate submissions or demonstrate compliance. It does not require the industry to implement a rigorous audit-trail record keeping system as prescribed in the proposed CROMERRR. Since the intent of the CROMERRR is to establish regulatory criteria for the industry to submit electronic reports, it should focus only on the "submission." The underlying data used to generate the "submission" have been properly regulated by the existing regulations and should not be changed by the CROMERRR. We recommend that the existing record keeping requirements remain unchanged for the industry that may elect to participate in the electronic reporting.

Many regulated facilities, especially medium to smaller ones, will probably not have the required information technology (IT) infrastructure and expertise nor the financial resources needed to generate the necessary protections for preventing document alterations, deletions, or copying of electronic signatures. It is likewise doubtful that they can develop capabilities for maintenance of unalterable and secure electronic documents and digital audit trails that demonstrate that prescribed protections have been effective. Costs to implement a record keeping system as required by the

proposed rule will be high and does not provide any environmental or regulatory benefits to the industry or states.

Delegated state agencies participating in electronic reporting should be charged with developing receiving systems which make electronic reporting cost effective and reduces reporting burden while meeting EPA security concerns. This would ensure a uniform record keeping "standard" and allow for a single point of maintenance, eliminating the need for the EPA to review and approve potentially numerous individual and separately designed systems.

At a minimum, the EPA should modify the preamble to state that the record keeping system requirements can be satisfied by systems maintained by either the receiving agency (delegated authority) or the regulated entity (facilities within non-delegated states). This should reduce industry concerns regarding the burden to implement and comply with these requirements.

3.100(a)(8) – The "required period of record retention" is not clear in the proposed rule. Record retention requirements should not be arbitrarily assigned but instead linked to a program cycle such as a five-year permit review process.

Subpart D – Electronic Reporting and Record Keeping under EPA Approved State Programs

3.1000(a) – If the EPA approved State, tribe, or local environmental program meets the requirements of this part, does it still have to be revised? This should probably be re-worded to something such as: (a) State, tribes, or local environmental programs that wish to receive electronic reports or documents in satisfaction of requirements under such programs must ensure that the EPA approved State, tribe, or local environmental program meets the requirements of this part.

3.1000(b) – It is suggested that the language be changed to state "the States, tribe, or local government must demonstrate, <u>in writing</u>, the electronic reporting..." As stated, the requirement could be interpreted to require a "hands on" or "live" demonstration of the functional system. In addition, the EPA should develop guidance specifying the format and examples of descriptions which would demonstrate how an electronic document receiving system will meet the requirements of this rule. This guidance document should also specify when and how EPA will approve the program revisions. It is recommended that any review take place early in the development/pilot process. The potential costs to change/retrofit an application are much lower at the design state as opposed to after a statewide implementation.

3.2000 – There are a number of issues pertaining to "acceptable electronic document receiving system" requirements discussed in the rule preamble but not in the proposed rule itself. These preamble issues, some of which the EPA would like comments on,

are discussed below in Section 3.2 and also later in the document under "Additional EPA Preamble Issues."

3.2000(a) – The seven proposed General System Security requirements, described in both the preamble and the rule, appear to be sufficient to ensure that the integrity and authenticity of the electronic documents it receives and maintains is adequate. Section 3.2000(1) and (2) both call for "robust protections" against unauthorized system access and use of electronic signatures without defining what "robust" means. This ambiguity needs to be resolved, either through definition or reference to other sections of the preamble and/or rule.

3.2000(5) – Could be restated as: 'Ensures that an electronic document can only be modified with detection once the electronic signature has been affixed.'

3.2000(d) - The submitter registration, renewal, and surrender language presented in pp. 46173-46174 of the preamble appears very cumbersome. While we can appreciate the intent of this language, perhaps it can be simplified. Another option is to consider the alternative posed in the preamble of adding a provision paralleling 21 CFR Section 11.100(c)(2) (under the Food and Drug Administration's electronic signature rule) requiring that signature holders upon request "provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature." Codifying such a provision is not recommended since the "language" should be a guideline used with some discretion, as long as the intent of the provision is adequately addressed.

We do support the EPA's proposed requirement that the electronic document receiving system have a mechanism to automatically revoke an electronic signature whenever (1) there is any evidence that the electronic signature has been compromised, and (2) there is notification from an entity that the holder of an electronic signature previously authorized... is no longer authorized... We also support that the same mechanism be in place if there is any evidence that the submitter has violated the registration agreement but only if the terms of the agreement are clearly defined.

3.2000(d)5 – The rule should not require periodic registration renewal. Those submitting a paper report are not required to "periodically" renew and therefore this requirement should not be imposed on those using electronic reporting. This could develop into a large burden on the system administrators, especially delegated states with a large number of facilities.

As an alternative, the rule should: "Require that the registrant renew if anything has changed since the last registration or renewal notice, etc."

The statement "... criteria of paragraphs (a) and (b) of this section are met, taking into account both applicable contractual provided and industry standards..." does not have

much meaning. What are the referred to "industry standards"? What industry and what process is required when the standards change?

3.2000(e)(1)(i) – This rule requires that the receiving system provide an onscreen review of the data "to be transmitted" and the associated contextual labeling information before the electronic signature can be affixed. This proposed requirement is unnecessarily burdensome since it is the reporting entity's responsibility for examining and understanding the content in order to certify its accuracy and completeness prior to signature. A user's ability to view the content of documents prior to certifications should be the same as viewing it after certification. More importantly, a receiving system should have the capability of allowing a participating facility to submit corrections and addendums to earlier submissions at some later date after on-line viewing from the receiving system. A submitting entity should also be able to remain on-line and view a submitted document after receiving notification that the submission has been received.

The state regulatory program should be given the discretion to require that electronic signatures and certifications be performed prior to submittal where the electronic submittal contains all the necessary data (and possibly contextual information such as monitoring requirements, if needed) that would normally be submitted on an approved paper form.

3.2000(e)(1)(ii) – The proposed rule states that a "certification statement that is identical to that which would be required for a paper submission of the document appears on-screen in an easily-read format immediately above a prompt to affix the certifying signature." The need for such a certification is undeniable, but we do not believe that the certification statement must be "identical to the one on the paper form. It should, however, be similar in context to allow for any additional information deemed necessary by the regulatory agency. Similarly, the exact location of such a statement on a page or form, while critical, should not be dictated by rule.

3.2000(e)(2)(ii) – The proposed statement "Is sent to an address whose access is controlled by password, codes or other mechanism that are different than the controls used to gain access to the system used to sign/certify and send the electronic document..." needs to be clarified. It is unclear if this means something as simple as an e-mail account or something more complex.

3.2000(e)(3) – We do not believe that the copy of record specified in (e)(3) needs to include all the warning, instructions and certifications statements presented to the signatory during the signature/certification process. All that should be submitted as the copy of record is the required data.

3.2000(e)(3)(iii) – The definition of "agency electronic signature" needs to be clarified and possibly eliminated from the technology-neutral intent of the proposed rule. Other technology based options may become apparent at a later date.

3.2000(f)(1) - The definition of "precise" routing needs to be further clarified in the preamble or explained in the rule. It is not clear what kind of information would be required or how precise the routing information would need to be. As Internet technology becomes more popular and affordable, it shall become one of the preferred methods by states to implement an electronic reporting system. Data transmitted via Internet will go through different routers and servers based on their availability at the time of transmission. If the proposed CROMERRR requires tracking of the "precise routing" of the data transmission, we feel that it not only will create an unnecessary burden to the servers, but also provides "no additional data security or environmental benefits" to the data. We agree that "reasonable data security" be required in the rule. We offer the following suggestions to address the data routing security:

1. The transmission is conducted in a server driven Secured Socket Layer (SSL) environment.
2. Additional information could be recorded at the server such as:
   - the user ID.
   - the TCP/IP address used by the user for the submission.
   - time when the data file was selected by the user on the submission screen.
   - time when the data file was sent by the user on the submission screen.
   - time when the data file was received by the server.
   - time when a receipt acknowledgement was sent to the user.
   - time when the data was processed by the server.
   - time when the final data processing result status was sent to the user.
3. All time stamps will be the server time.

The routing description and its associated "precision" may be technology dependent and require the electronic "copy of record" to include "all warnings, instructions and certifications statements presented to the signatory during the signature/certification scenario..." As previously stated, the need for "all the warnings, instructions...." as referenced in 3.2(e)(3), to be stored by the regulatory agency, the original source for this information, should not be a requirement.

3.3000(b) – In order for the EPA to approve a program revision under paragraph (a), the State, tribe, or local government must demonstrate that the records maintained meet the criteria established in this rule. The time and form of the demonstration should be clarified. The rule should specify when and how the EPA would approve the program revisions.

We strongly feel that the format of the approval process should be determined by the states, the process should be streamlined, and most importantly, must consider the fact that certain states, including Michigan, have already implemented or are in the process of implementing electronic reporting systems. States already in the implementation stage of any electronic reporting systems prior to the final rule promulgation should be given the flexibility to offer "alternative standards" to the final requirements, if the

alternatives are "reasonably achievable" within their system design. The alternative standards should be part of the review process and should not require prior approval from the EPA. If "alternative standards" are not feasible to implement within the existing systems, the state systems should be considered "grandfathered" systems and be exempt from any difficult-to-achieve requirements as long as the implementation difficulties could be demonstrated to the EPA.

The MDEQ has heard from a number of individuals from the regulated community regarding the costs associated with the rule and the concerns that the rule is not voluntary but mandatory due to the current submittal of electronic reports. They are concerned that if the rule is finalized as proposed, current electronic reporting will not be allowed or recognized by the EPA unless the State meets the EPA's criteria as a receiving system. Although proposed as a voluntary system, States currently accepting electronic submittals would either need to revert to a paper based system or modify their receiving systems to comply with the EPA prescribed model.

The other main area of concern is the proposed record keeping requirements which have the potential to be very costly and onerous to industry. Regulated facilities currently keep most of their environmental records in an electronic format. The proposed rule would require that the states disallow all electronic record keeping until the state adopts and the EPA approves the programs that incorporate the EPA's criteria for record keeping.

The language in 3.3000(b) should be modified to read that "the regulatory entity demonstrated this capability in writing that records maintained electronically..."

Additional EPA Preamble Issues:

Issue: – See 66 FR 46174: Whether the EPA should require a surrender certification statement to attest compliance with the Electronic Signature Agreement whenever a person leaves a position or otherwise surrenders their electronic signature.

Response: This requirement is not practical and not enforceable by the regulatory agency due to the lack of intimate knowledge of the personnel changes within a regulated entity. The MDEQ suggests a surrender certification statement not be included in the rule.

Issue: – See 66 FR 46175: Whether EPA should include any of the types of "Warnings" as suggested in the preamble discussion.

Response: Keep on-screen "Warnings" to a minimum.

Issue: – See 66 FR 46180: One of the key CDX Building Blocks specifies the use of digital signatures based on PKI for electronic submissions. This building block is

"meant to ensure that CDX can perform the functions of an electronic document receiving system under the proposed rule."

Response: In many instances, the electronic submission will not require a PKI level of security. Delegated states should be given the discretion of using alternative technologies and administrative controls which demonstrate the intent of this rule. For example, appropriate security can be achieved with the combination of the (1) submitter registration process, (2) user names, PIN, and password combinations, and (3) secure socket layer. Requiring specific technologies contradicts the rule's "technology-neutral" intent.

The cost of PKI implementation is too high to be considered practical on a large scale. The EPA's own annual estimate to implement and operate electronic reporting and record keeping, as stated in FR 46178, is $1.1 million per year per state and $1,140 per facility. A significant portion of this, based on in-house estimates, is for digital signatures based on PKI. This high cost may serve as a major disincentive towards participation in electronic reporting. Accordingly, in keeping with the intent of the rule to remain technology-neutral and due to the financial and administrative burdens, the requirements to use digital signatures based on PKI should be removed.

In conclusion, the MDEQ recommends the proposed rule be withdrawn and revised to address these issues which would ease the burden of regulatory reporting and record keeping.

Should you require further information, please contact Ms. Lynn M. Draschil, Chief Information Officer, at 517-241-7423, or you may contact me.

Sincerely,

Russell J. Harding
Director
517-373-7917

cc: Mr. Gary R. Hughes, Deputy Director, MDEQ
Mr. Arthur R. Nash Jr., Deputy Director, MDEQ
Ms. Lynn M. Draschil, CIO, MDEQ